IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

A Continuous Authentication Approaches for Data Security Services against Reconstruction Attacks using Multiple Biometric

Mrs. S. Gunasundari M.Sc., M.Ed., M. Phil[1], Miss. R. Punitha[2]

Assistant Professor, Department of Computer Science, Sakthi college of Arts and Science for Women, Oddanchatram[1]

M. Phil Scholar, Department of Computer Science, Sakthi college of Arts and Science for Women, Oddanchatram[2]

Abstract: Internet Security and data privacy is preserved by the appropriate authentication schemes. User name and password based authentication is the fundamental step to access internet services. The conventional authentication system follows initial session verification rather than continuous verification. The continuous authentication is referred as the detection of authorized users and authenticating them even after successful login. This type of continuous authentication technique plays vital role in internet security as it performed by various types of authentication schemes. In this paper, a complete authentication protocol is used, which focuses on the throughout authentication scheme that is from login to logout time. This system about the authorized person's face detection for throughout session (From login time to logout time).The Web camera placed in front of the system in which they are working that camera will capture the face of the authorized person if the person start to move from the camera the capturing process will struck and the transaction will not allow the unauthorized persons to work. This application is fully applied with the camera. Once the person wants to do the transaction then he should sit in front of the camera and the face is authenticated for further steps. The camera will continuously monitor the face to avoid in authenticate transactions. If the user tries to move from the camera then the transaction will not be continued. It will get struck. So, user should be there until he/she finishes the transactions. This project utilizes face matching algorithm and canny and sobal algorithm for edge detection.

Keywords: Face matching, Finger print recognition, authentication, Internet Security, biometric techniques, continuous authentication.

I. INTRODUCTION

Data security and secure User authentication is an ultimate goal of almost all applications. All application has the aim to authenticate user for secure data access. This yearned lots of attention due to the recent boosting in the frequency and complexity of cyber-attacks. Nowadays authentication systems are grown with different types of working procedures and attribute against those attacks. In traditional authentication system, username and passwords are used for authentication. All authentication techniques such as biometric, device based and graphical passwords are used at the time of login, there is no verification performed during the session. In some traditional web mail servers such as Yahoo, used active screen monitoring technique [1]. This allows the users to logout the session if they are inactive. This type of traditional method avoids unauthorized access in the website. The services will be provided after successful authentication and the resources will be available for a fixed period of time. This kind of authentication is typically based on single session verification. This approach believes that a single verification, when performed at the beginning of the session is sufficient, and that the identity of the user is constant during the whole session. So there is a need to develop a continuous verification for secure throughout the session. In this paper, we surveyed various techniques and tools used for web security.

Internet security consists of the procedures adopted to monitor and prevent authorized entry in remote a computer network. Internet security involves the authorization of access to data in a distributed manner, which has more challenges in the real time phenomenon. Internet security begins with basic username and password verification. This type of verification only consist the password field, this type of authentication is known as single factor authentication. Security management for internet is different from the normal desktop security application [2]. A desktop application security only requires basic security when comparing with the internet applications, this type of applications needs strong techniques along with new hardware support to thwart hacking and other types of attacks [3]. To resolve this issue, we need continuous user authentication methods that continuously monitor and authenticate users based on some biometric elements. Earlier mechanisms for continuous user authentication cannot authenticate users without biometric observation, so biometric authentication is useful for continuous authentication. In such application, the continuous user authentication to be easy

DOI 10.17148/IJARCCE.2017.62109

to use, passive authentication is desirable because the system should not require users' active cooperation to authenticate users continuously. The passive authentication is using faces as default continuous verification.

Need for Authentication
Authentication is the process which allows a user to validate their self before accessing their data. If the server and client cannot properly authenticate, there is no belief in the actions on information provided by their part. Authentication can involve highly hard and tricky methods to provide high level security. The simplest form of authentication is the one factor authentication, which stated above.

1. **Frequency of security contravention:** in real time internet applications and social networks such as twitter, Facebook and linked in have R&D departments, which captures and monitors the authentication and access activities [4].

2. **Enhanced methods of authentication** have "morphed from traditional tokens to USB devices to smart cards to fingerprint readers, soft tokens and scanning devices." Contextual authentication, based on analytics of behavior patterns and device patterns, is growing in importance and more vendors are offering it with their core user authentication products. In addition, there is an increased interest in using biometrics for a higher level of assurance with improved user experience, including form factors like voice recognition, iris matching, finger and other biometric features [5].

1.1 Role of Continuous Authentication

Continuous authentication is important not only for high security systems, but also low security systems. For example, an average user typically walks away from the computer for short breaks without logging out of the system. This opens up an opportunity for unauthorized users to access the computing resources easily. We evaluate the following three criteria for continuous user authentication [6].

1. Usability: The system should not require any additional verification for second time as long as the users are in front of the device. In such cases the system can't re-authenticate the user with any other biometric observations other than the face and posture. For example, it would be inconvenient for the user to meet the requirement of entering a password or provide his fingerprint whenever he takes a break to read a book or consult notes.

2. Security: The system should require active re-authentication of the user every time the user walks away from the application or system. This requirement will ensure that unauthorized users cannot access the resources after the legitimate user moves away.

3. Cost: In continuous authentication, cost is the important factor, because the remote system should possess proper hardware to complete the multi factor authentication and continuous authentication schemes. For this reason, the authentication system should use only the standard devices and avoid the use of high cost devices.

3. Internet Security through Biometrics:

Biometrics is the science of establishing identity of an individual based on the physical or behavioral attributes of the human. The relevance of biometrics in modern society has been reinforced by the need for large-scale identity management systems whose functionality relies on the accurate determination of an individual's identity in the context of several different applications over internet. Additionally, biometric authentication systems can be more convenient for the user which doesn't need to memorize, it achieves the privacy and a single biometric component can be used to access several accounts [7]. Some types of biometric data are illustrated below.

a. Physical biometrics based authentication
b. Behaviour based authentication

a. Physical biometrics based authentication

Face Biometrics:
Face detection and recognition includes many complementary elements, each part has its own. Depending on regular system each part can work individually. Face detection is an image processing concept that is based on learning algorithms to allocate human faces in digital images [8]. The biometric data's such as face matching and finger matching application need to be performed the following steps

- Face ,finger Recognition
- Feature extraction, and
- Face and finger matching
- Authentication.

Fingerprint Scan Biometrics:
Fingerprints are the common and widely used biometric component for almost all application. Due to it reliable nature, it is used in all application. When comparing with other biometric components such as iris, palm print or voice biometric the finger prints are easy to scan and match. So this is very useful with fast matching. The advancement of fingerprint can be recognition of veins and nerves with the help of high quality scanners [8]. This is unique and also we have numerous choice i.e., human have ten fingers. The user can use any finger among ten.
The following fig 1.0 shows the basic process associated with the biometric scanner system. The initial process of this system is feature extraction, there are several feature extracting techniques are available in the current research. We left the comparison of those techniques for future work. We examined different techniques and methods used in continuous verification.

DOI 10.17148/IJARCCE.2017.62109

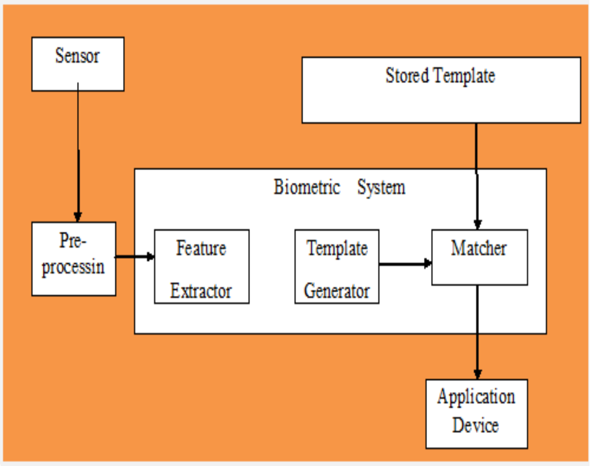

FIG 1.0 fingerprint scanning system architecture

In literature [9] there are several authors from the papers [10][11] have highlighted several security threats in biometric authentication, in order to eliminate the fake entry in biometric based authentication, Derakhshani et al. Proposed two software-based for fingerprint liveners detection, this also includes the other active parameters to match the fingerprint [12]. Soutar proposed a “hill-climbing” attack for a simple image recognition system based on filter based correlation. Using the matching scores returned from the matcher that was generated for each of the successive face images, this initial image is modified.

b. Behavior based authentication:

Keystroke Biometrics:
Keystroke biometrics or monitoring keystroke dynamics is considered to be an effortless behavioral based method for authenticating users which employs the person’s typing patterns for validating his identity [13]. Keystroke dynamics is “not what you type, but how you type.” In this approach, the user types in text, as usual, without any kind of extra work to be done for authentication. Moreover, it only involves the user’s own keyboard and no other external hardware. All keystroke dynamics studies involve conducting five main experiment parts in the following order: recruiting participants, requesting a typing task to be done by the Participants, collecting the timing data of keystrokes, obtaining timing features from the raw keystroke data, training the classifier using part of the keystroke data and using the other part for testing the classifier [14].

c. Device based authentication

User authentication using devices are referred as more flexible and reliable way of verification, which fights against keylog and other types of attacks. Initially the devices such as mobile phones are used to fight against these password threatening attacks. Users should carry and have their mobile phones at the time of authentication. The OTP (one Time Passwords) are the popular technique, where user should poses their phones. The received keys will be taken for authentication. This types of authentication is known as device based authentication [15].

II. LITERATURE

The idea of continuous authentication is not novel approach. But the criteria and components are different and innovative. The differences are identified between biometrics and traditional passwords are discussed by Klosterman and Ganger in [16], they have also examined the proved biometrics are the most appropriate way to achieve continuous authentication. In order to prove, that Linux Pluggable Authentication Module (PAM) [17] has been proposed. This technique increased the computational cost, the authentication decision became very slow and face was used for verification.

Later from biometric components, voice, face and fingerprints are used for continuous verification [18]. The author found two key issues in continuous authentication such as the integration of time and modality, and the authenticity certainty at any time. But the work only focused the multi component fusion and they didn’t study the consequences of detection process. And the approach is failed to satisfy the cost criteria.

Later the first implementation of a continuous verification system integrated into an operating system (OS) is proposed in [19], in this paper the author integrated the OS and biometric verification components. They have used camera and fingerprint component. The integrated portion of finger with mouse increases the reliability, however this method is not satisfied the scalability oriented implementation. The above modalities are very accurate; but they might be inherently limited in their sampling rate.

By continuous verification, the identity of the human operating the computer is continually verified at every session [20]. Verification is computationally simpler than identification and attempts to determine how “close” an observation is to a known value, rather than finding the closest match in a set of known values. Verification is a realistic operation in the normal usage of a computer system because we can assume that the user’s identity has been incontrovertibly established by a preceding strong authentication mechanism. It is also appealing because it can conceivably be offloaded to a hardware device that is properly initialized with user specific data upon successful login.

A model-based evaluation of scalability and security tradeoffs of a multi-service web-based platform has been proposed. This utilizes the continuous evaluation of security mechanism, this degrades the performance properties. The different configurations are assessed and the security counter measures are introduces in this paper [21].This paper highlights one emerging application of stochastic modeling, i.e., the evaluation of the impact of security countermeasures on the performance of a service-based architecture such as SAAS (software as a service). This paper left several process as future work. Such processes are handling attack models, providing balanced security and the performance criteria's. The author failed to evaluate the proposal based on the above scenario.

D.M. Nicol, W.H. Sanders, and K.S. Tridevi [22] surveyed existing model-based techniques for evaluating system steadiness, and summarized the need of system security. The authors found that many techniques from dependability evaluation can be applied in the security domain later however that significant challenges should made appropriately. The system concentrated on the cyber attacks and the impact of those attacks in the continuous verification. But still there is no solution for unknown vulnerabilities.

III. PROPOSED SYSTEM

1. Enrollment Module

The registration module contains all the information about the person. It actually captures image of the person through Webcam and stores all the relevant details of the person such as name, phone number along with the fingerprint. The following figure describes an access control system based on fingerprint authentication. In this model, each user has an account and a corresponding ID in the Database.

2. User authentication:

User credentials are registered and stored with the fingerprint images. The registered user is the valid person to do the application. Other persons cannot access the application even they steal the credentials of the valid persons.

3. Biometric data Identification and Verification Module

Users are identified by their measurable human characteristics, such as fingerprint. Biometric characteristics are believed to be a reliable authentication factor since they provide a potential source of high-entropy information and cannot be easily lost or forgotten. Despite these merits, biometric authentication has some imperfect features. Un-like password, biometric characteristics cannot be easily changed or revoked. Some biometric characteristics (e.g., fingerprint) can be easily obtained without the awareness of the owner and it will forward and stored in database.

a. Fingerprint Matching:

Fingerprint matching algorithm that initially identifies the candidate common unique (minutiae) points in both the base and the input images using ratios of relative distances as the comparing function. A tree like structure is then drawn connecting the common minutiae points from bottom up in both the base and the input images. Matching score is obtained by comparing the similarity of the two tree structures based on a threshold value. Fingerprint based biometric authentication and verification systems have gained immense popularity and acceptance ever since their inception. Matching two fingerprints can be unsuccessful due to various reasons and also depends upon the method that is being used for matching. Very popular methods include minutiae based matching, correlation based matching, pattern matching etc…

Matching Techniques:

The three matching techniques are

- direct matching
- minutiae matching

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. The endpoints and crossing points of ridges are called minutiae. A ridge ending is defined as the ridge point where a ridge ends abruptly. A bifurcation is defined as the ridge point where a ridge bifurcates into two ridges. It is a widely accepted assumption that the minutiae pattern of each finger is unique and does not change during one's life.

b. Face recognition and matching

In face identification module, if the person enters the image of that person is compared with the image that are stored already in the database. In face verification module, if a person enters User will be verified whether they are authorized user or an unauthorized user. This is very useful to monitor who visited often. Face recognition systems in general, and access control systems based on face authentication in particular, use a "learning" mechanism to collect data on facial characteristics if users. Hence, the first important point to care about in a face recognition model is the Face Database storing this information. When the system finishes scanning a video or photo of a user's face, the digitalized information will go through these following modules one after another:

- Face Detection: locating the face in the photo or video and removing unnecessary details on the background.
- Feature Extraction: extracting facial characteristics needed for recognition.
- Feature Match: comparing scanned information with database to decide if it matches some user's face. If the face matched, the ID of the corresponding is returned.

Edge detection –canny sobal algorithm

4. Continuous Verification for security:

The camera will continuously monitor the face to avoid in authenticate transactions. If the user try to move from the camera then the transaction will not be continued. It will get struck. So, user should be there until he/she finish the transactions.

a. Face monitoring using camera:

This application is fully applied with the camera. Once the person wants to do the transaction then he should sit in front of the camera and the face is authenticated for further steps.

DOI 10.17148/IJARCCE.2017.62109

5. Transaction maintenance and Report:
In this transaction maintenance all the transaction details will be updated and monitor in a secure manner. So the information will not misuse by other persons.

In accessibility module, if a person is an authorized user, then User will be permitted to access the resources. Otherwise, User will not be permitted. This provides more security and prevents from unauthorized user by providing face recognition.

In this report **"**Login to Logout authentication for all online Transactions "all the information are in secure way and information are updated ,final report is generated.

6. Intruder alert Process:
If the authentication fails, the system automatically finds the system details and captures the faces of users. These details will be send to the user via email.

Architecture:

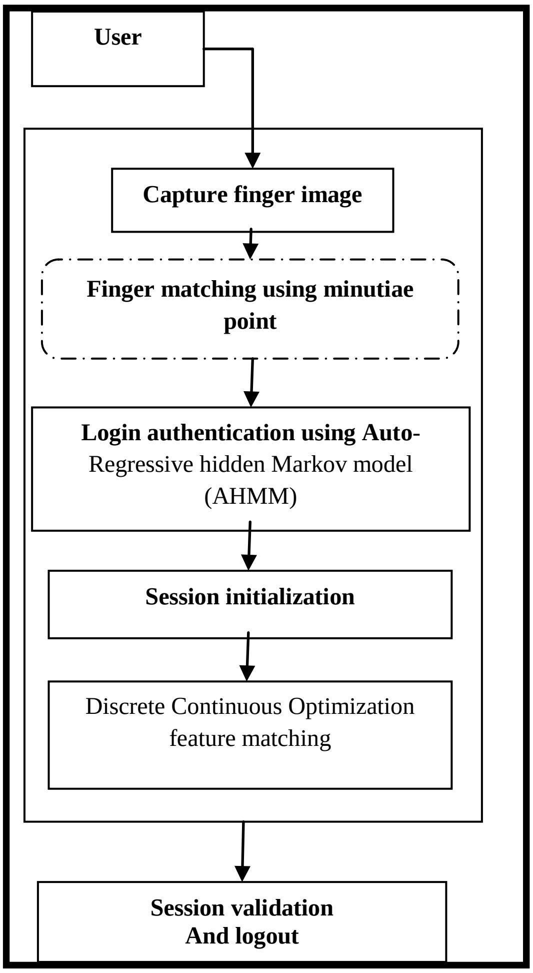
User
Capture finger image
Finger matching using minutiae point
Login authentication using Auto-Regressive hidden Markov model (AHMM)
Session initialization
Discrete Continuous Optimization feature matching
Session validation
And logout

Fig 1.0 proposed system architecture

III. CONCLUSION

In this paper we presented an empirical study about the continuous authentication in internet services. From this survey we could identify different problems and issues associated with the continuous verification. Many authors proposed different modality and biometric components to achieve continuous verification, but only few concentrated on the cost criteria. And such studies are size limited and created many scalability issues. From this survey we have found several future directions to improve the authentication system in real-time internet services.

REFERENCES

[1] A. Klosterman and G. Ganger, "Secure Continuous Biometric-Enhanced Authentication," Technical Report CMU-CS-00-134, Carnegie Mellon Univ., May 2000.

[2] A.G. Morgan, "The Linux-PAM System Administrators' Guide," documentation distributed with Linux-PAM, http:// www.kernel.org/pub/linux/libs/pam/pre/library/, 2006.

[3] A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics," Proc. Workshop Multimodal User Authentication, pp. 131-137, 2003.

[4] S.Kumar, T.Sim, R.Janakirman, and S.Zhang, ''Using Continuous Biometric Verification to Protect Interactive Login Sessions,'' Proc. 21st Ann Computer Security Apllications Conf. (ACSAC' 05), pp.441-450, 2005.. Continuous Verification Using Multimodal Biometrics

[5] L. Montecchi, N. Nostro, A. Ceccarelli, G. Vella, A. Caruso, and A. Bondavalli, ''Model-based Evaluation of Scalability and Security Tradeoffs: a Case Study on a Multi-Service Platform'' Electronic Notes in Theoretical Computer science, vol.310, pp.13-133, 2015.

[6] D.M.Nicol, W.H. Sanders, and K.S. Tridevi, ''Model-Based Evaluation: From Dependability to Security,''IEEE Trans. Dependable and Secure Computing, vol. 1, no.1, pp.48-65, Jan. – Mar. 2004.

BIOGRAPHIES

Mrs. S. Gunasundari M.Sc., M.Ed., M Phil. is working as Assistant Professor of Computer Science department in Sakthi college of Arts & Science for women. Her teaching experience in 4 years and her area of interest is Digital image processing.

Miss. R. Punitha completed MCA in PSNA College of Engineering and technology and currently pursuing M. Phil in computer science in Sakthi college of Arts & Science for women. She worked two years programmer in Neolysi Technology, Chennai. Her area of interest is Network security and web mining.